

IMPORTANT CLIENT NOTICE

02.01.22

Be on the Lookout for Phishing Scam Emails

Beware, it's phishing season! "Phishing" is the attempt to acquire confidential information, often for malicious reasons, by impersonating a trustworthy individual in an email message. Phishing is thought to be one of the most dangerous methods of cybercrime because it cannot be detected by antivirus software programs.

These extremely sophisticated email scams are increasingly popular during tax season. Cyber criminals will pose as company executives or other legitimate members of the leadership team and then request proprietary employee and/or company information. The emails often appear harmless since they look like they are being sent from the company's email domain. Cyber criminals can easily access enough information to be dangerous and damaging to your organization. It is important to be aware of the recent phishing schemes, below is an example of an email we have seen sent to a number of clients and to HR Knowledge:

Greetings

How much is my estimated gross pay for the year 2022? Can i send you my new Direct Deposit information or voided check for you to change on records?

Warmest Regards,

[Your CEO's name here]

In the above request, notice there are punctuation and grammatical errors. This is one of

This content is provided with the understanding that HR Knowledge is not rendering legal advice. While every effort is made to provide current information, the law changes regularly and laws may vary depending on the state or municipality. The material is made available for informational purposes only and is not a substitute for legal advice or your professional judgment. You should review applicable laws in your jurisdiction and consult experienced counsel for legal advice. If you have any questions regarding this content, please contact [HR Knowledge](#).



the highlights that the Federal Trade Commissions has published in their [tips on how to avoid phishing scams](#).

It is important that employers take steps to educate their team on how to properly handle these emails, including notifying the Federal Trade Commission (FTC). Remind your employees to never respond to any request, or click on any links, that seems out of the ordinary before calling the person to confirm that they made the request.

If you got a phishing email or text message, report it. The information you give can help fight the scammers.

Step 1. If you got a phishing **email**, forward it to the Anti-Phishing Working Group at reportphishing@apwg.org.

If you got a phishing text message, **forward it to SPAM (7726)**.

Step 2. Report the phishing attack to the FTC at [ReportFraud.ftc.gov](https://www.ftc.gov/identitytheft).

Most importantly, take the time to educate your staff. **This is especially important for your payroll and HR employees who are privy to sensitive and confidential information.**

The People Simplifying HR

For almost twenty years, HR Knowledge has made it our mission to demystify the complex and daunting process of HR management. We do more than just provide the level of service and technology you'd expect from an industry leader. We combine unparalleled passion for service with our decades of HR, payroll, and benefits experience to provide our clients with personalized and actionable advice that is second—to—none. From managed payroll to employee benefits to HR support, we can help your organization thrive, grow, and reduce operating costs—no matter what industry you serve. Whether you're interested in our Full-Service solution or just need your employee handbook written, HR Knowledge can help you minimize risk while staying on top of compliance regulations. The bottom line? We're not just another cloud-based technology company that also does HR, #WeAreHR. [Get the scoop](#) on how we can help you simplify HR.



@WEAREHRK